5998-4022 5.5.5.0

MSM7xx, MSM3xx, MSM4xx 5.5.5.0 Release Notes

Contents

General information

Online documentation

You can download documentation from the HP Support Website at: www.hp.com/support/manuals. Search by product name or part number.

Terminology

In this document, the generic term “controller” may be used in place of MSM7xx Controller product names and the generic term “AP” may be used in place of MSM3xx / MSM4xx AP product names.

Applicable products

This document applies to these HP MSM7xx Controllers:

Model	Part
MSM710 Access Controller	J9328A
MSM710 Mobility Controller	J9325A
MSM730 Access Controller	J9329A
MSM730 Mobility Controller	J9326A
MSM750 Access Controller	J9330A
MSM750 Mobility Controller	J9327A
MSM760 Access Controller	J9421A
MSM760 Mobility Controller	J9420A
MSM765zl Mobility Controller	J9370A

This document applies to these HP MSM3xx / MSM4xx APs:

Model	WW	Americas	Japan	Israel
E-MSM430	J9651A	J9650A	J9652A	J9653A
E-MSM460	J9591A	J9590A	J9589A	J9618A
E-MSM466	J9622A	J9621A	J9620A	J9619A

Model	WW	USA	Japan	Israel
MSM310	J9379A/B	J9374A/B	J9524A/B	
MSM310-R	J9383A/B	J9380A/B		
MSM317	J9423A	J9422A	J9423A	
MSM320	J9364A/B	J9360A/B	J9527A/B	
MSM320-R	J9368A/B	J9365A/B	J9528A/B	
MSM325	J9373A/B	J9369A/B		
MSM335	J9357A/B	J9356A/B		
MSM410	J9427A/B	J9426A/B	J9529A/B	J9616A
MSM422	J9359A/B	J9358A/B	J9530A/B	J9617A

Note: The E-MSM430, E-MSM460, and E-MSM466 APs are also known respectively as MSM430, MSM460, and MSM466.

Note: “WW” identifies worldwide versions for all other MSM-supported countries except the Americas, Japan, and Israel.

Software Updates and Licensing portal

The Software Updates and Licensing portal provides access to the latest software updates to customers with a support contract. An HP Passport is required to access the Software Updates and Licensing portal at www.hp.com/go/hpsoftwareupdatesupport and available to customers that have purchased a maintenance and support agreement.

Updating software

Controllers

Update the controller software as described in the *Software updates* section of the *MSM7xx Controllers Management and Configuration Guide*. After the controller is updated, it automatically updates all of its controlled devices to the same software version.

Autonomous APs

(Not applicable to MSM317.) For autonomous APs, update the software as described in the *Software updates* section of the *MSM3xx / MSM4xx Management and Configuration Guide*.

About Rev B MSM APs

As of July 1, 2010, Rev B MSM APs are available. This applies to the Rev B version of the following MSM APs: MSM310, MSM310-R, MSM320, MSM320-R, MSM325, MSM335, MSM410, MSM422.

Rev B MSM APs (product number ends with the letter “B” as in “J9xxxB”) ship from the factory with at least software v5.3.5 pre-installed. Rev B MSM APs cannot be downgraded to earlier versions of v5.3.x software. Therefore when adding a Rev B MSM AP to a network of controlled APs, the MSM7xx Controller must be running at least software v5.3.5, otherwise the Rev B MSM AP will not be recognized by an MSM7xx Controller. Only MSM7xx Controllers and MSM Access Points that are covered by a software Care Pack or software Contract can be upgraded from v5.3.*x* or 5.4.*x* to v5.5.x. Please contact HP Support for entitlement determination and download instructions. Support contact information is available on the HP Support Web page at: www.hp.com/networking.

RF Manager software and MSM software version compatibility

RF Manager versions 5.9.x and 6.0.x work with MSM software version 5.5.x and higher. However, to use the WLAN Integration feature in RF Manager 6.0.x, the RF Manager and MSM software versions must be matched as follows:

MSM7xx software version	Compatible RF Manager Sensor devices version version(s)	Sensor devices version	
		Sensor-only devices (MSM415)	AP/Sensor devices (MSM320*, MSM325, MSM335)
5.5.5.0	6.0.177 or above	Upgraded automatically by RF Manager	Upgraded automatically by MSM7xx Controller
5.5.3.x	6.0.157 or above		
5.5.1.x/5.5.2.x	6.0.154 or above		
5.5.0.x	5.9.203, 6.0.147 or above		

*MSM320 APs that have been upgraded to MSM325 RF sensor via HP MSM320 RF Sensor License J9384A.

Note: If with RF Manager 6.0.x you choose to use mismatched software versions, you should first turn off the WLAN Integration in RF Manager.

Note: Upgrading an MSM7xx Controller to v5.5.5.0 will also automatically upgrade any MS325 and MSM335 Sensors it manages to v5.5.5.0.

Note: The MSM415 Sensor has no MSM software dependency. It is managed and upgraded directly by RF Manager.

Information for PCM and PMM software users

PCM 3.20 and PMM 3.10 software supports MSM devices as follows:

- Full support of MSM devices at software version 5.4.2.0 or higher.
- Limited support of MSM devices at software version 5.3.x and 5.4.0.
- No support of MSM devices at software version 5.4.1.

Note: Purchase of PCM 3.20 and/or PMM 3.10 does not entitle you to an upgrade for MSM products. Only MSM products covered by a care pack or contract that includes software upgrades are entitled to upgrades.

Fixes

The following issues have been fixed since the previous release:

ID	MSM7xx	MSM3x4x	Description
118445	✓		When using Subnet-based mobility, wireless clients my be unable to get an IP address. Note that Subnet-based mobility is already documented as deprecated with advice given to use MTM (Mobility Traffic Manager) instead.
118025	✓		The controller fails to send RADIUS requests to the secondary RADIUS server when the primary server does not respond.
116303	✓		In rare cases, wireless clients using Mobility Traffic Manager (MTM) have connectivity issues due to high CPU usage on the AP.
113415	✓		When the system time is set manually, if the team manager controller is shut down (power disconnected) when the team manager controller returns, the team manager controller time is set to the last saved time, which may cause team member controllers to fail to re-synchronize with the team manager controller.
111782	✓		When a VSC is configured to use 802.1X and an egress VLAN, a wireless client roaming from one AP to another may end up on another VLAN that is not the one configured for egress.
110850	✓	✓	AP names longer than 13 characters are not displayed properly on some management tool pages.
110731	✓		When payment services are configured and used, a duplicate payments page remains open for two hours instead of 30 seconds.
110632	✓	✓	(Applies to autonomous APs.) The Country code cannot be set using the CLI.
110479	✓		(Applies to E-MSM430, E-MSM460, E-MSM466.) If you set more than one WEP key only the first key will be used due to hardware limitations.
109938	✓	✓	The use of the % character is not allowed in the WPA pre-shared key.
109858	✓		(Applies to MSM760.) The Internet port cannot be manually set to 10 Mbps full duplex. Auto settings work as expected.
109750	✓		When the controller internal RADIUS server is under heavy load (200 or more users authenticating simultaneously), RADIUS authentication fails for some users. A message similar to this appears in the system log: `...radius exceeds data memory.`
109667	✓		Attempting to configure an SNMP v3 user with SHA/AES encryption will fail for some SNMP queries.
109633	✓	✓	(Applies to E-MSM430, E-MSM460, E-MSM466.) The data rate cannot be set with the CLI to rates MCS16 to MCS23.
109176	✓		APs located 16 or more hops away from a DHCP server may become unreachable by the controller due to timeouts.

ID	MSM7xx	MSM3x4x	Description
109130	✓		When using the internal RADIUS server, the controller does not keep track of queued EAPOL requests, causing some clients to be unable to authenticate.
109122		✓	(Applies to when Country is set to **Japan** for MSM410, MSM422, E-MSM430, E-MSM460, E-MSM466.) Channels 120, 124, and 128 do not have the same power settings as other channels in the W56 band.
108939		✓	When Security filters are not enabled in a VSC, wireless clients connected to the same VSC and with the same egress VLAN, cannot communicate with each other.
108553	✓		Active Directory authentications are not following the trust-relationship between servers.
108507		✓	(Applies to MSM422, E-MSM430, E-MSM460, E-MSM466.) A static Local Mesh link between any of these APs does not function correctly.
108397		✓	(Applies to Autonomous APs.) SNMP frequently restarts.
108189		✓	(Applies to E-MSM430, E-MSM460, E-MSM466 with clients that have UAPSD enabled (Unscheduled Automatic Power Save Delivery) enabled.) When wireless clients upload large files through the AP, the radio stops working until the AP is restarted.
107642	✓	✓	(Applies to Country=**Egypt**.) The HT40 channel is not available.
107455	✓		(Applies to 802.1X authentication with local RADIUS server.) Sessions time out too quickly, requiring users to re-log in.
107386	✓		When wireless clients authenticate with an external RADIUS server with the controller acting as a RADIUS client, the controller generates duplicate RADIUS ID in the packets, causing the RADIUS server to terminate the user session.
107224		✓	When there are usernames longer than 96 characters, the Wireless client Overview page stretches the Username column, making other columns unreadable.
106730	✓		(Applies to MSM710.) The controller reboots due to a memory leak caused when multiple wireless clients are performing a file transfer. A message similar to the following appears in the system log: `warning kernel Softdog, warning kernel cpu: 100%, warning kernel, cause 1`
106535	✓		When using **Always tunnel client traffic** in a VSC or when a controlled AP is L3 connected (tunnel is forced) and the AP is controlled through a local mesh link, the wireless clients that associate with the AP (that is bound to the VSC) will not have IP connectivity if **Allow traffic between: NO wireless clients** is selected in the VSC.
106509	✓		When the PRIMARY-WEB-SERVER-STATUS-URL or the SECONDARY-WEB-SERVER-STATUS-URL are configured for a user account profile, after authentication, the user is not forwarded to external web-sites.

ID	MSM7xx	MSM3x4x	Description
106458	✓		When 802.1X user statistics are being generated, unexpected messages similar to the following may appear in the system log: `eapolserver: assert: ieee802dot1x_stats.c IEEE802dot1xServer_PostStats 95`
106367	✓		When using Active Directory (AD) running on Windows 2008R2, access controlled users fail to be authenticated when a team member controller has taken over for the team master controller.
105875	✓		When the number of Mobility Traffic Manager (MTM) clients grows beyond 500, some of the APs may restart. A message similar to the following appears in the system log: `warning monitord monitord: CN13DLL03G Unexpected termination for process 'iappd -d -m 169.254.0.1 -t 10.14.0.36' [pid 29720, up for 2 sec(s)]`
105793	✓		When attempting to add a controlled AP, the CLI command **product type** does not work.
105736	✓		If an AP is set to use a country code where the 20/40MHz automatic channel width selection is allowed, and then the AP gets changed to another country code where the 20/40MHz setting is not allowed, the controller fails to recognize and synchronize the APs.
105574	✓	✓	When a WPA2 Enterprise wireless client disassociates, the AP incorrectly adds the following warning message to the system log: `warning eapolserver: <Access Point ID> Unable to update Interim Traffic (mac-address=<client MAC address>).`
105100	✓		When the country code is set to Turkey, teamed controllers are not able to synchronize.
105494	✓		The web-based management tool becomes unreachable and causes controller restart.
105448		✓	(Applies to E-MSM430, E-MSM460, E-MSM466.) Due to an internal error, the AP restarts. A message similar to the following appears in the system log: `Msg:dpr:Fatal exception in interrupt nip=c033dc80 lr=c033ebe4 sp=cd5f5790 trap=300 msr=29000...`
105370	✓		SOAP call **ControlledNetworkGetWirelessAssociatedClientStatus** made to the controller returns error **`Internal Error 1003`** for the client MAC address connected on radio 2.
105135	✓	✓	When a wireless client leaves the VSC without terminating the session, the location aware server does not confirm the session termination and a excessive number of messages similar to the following appear in the system log: `Discarded disassociation notice request due to session-id not matching the current user's session-id. Discarded disassociation notice request due to user not being associated.`
105023	✓		When an 802.1X authentication client egresses to a VLAN dynamically assigned from a RADIUS server and then the client roams between APs, after the roaming, the client is no longer able to reach the VLAN and it does not get an IP address lease.

ID	MSM7xx	MSM3x4x	Description
105005	✓		If the controller is configured for static NAT mapping, the **Extend ingress to egress interface** option on the DHCP relay configuration page does not work.
104910	✓		When configuring an AP with two Mobility Traffic Manager (MTM) VSCs with the same settings but different names and SSIDs on radios 1 and 2 respectively, clients lose connectivity when roaming between radios.
104761		✓	(Applies to autonomous E-MSM430, E-MSM460, E-MSM466.) Traffic cannot flow between wired and wireless clients through a local mesh link.
104601	✓		When the number of simultaneous connected clients approaches the maximum number permitted, high CPU utilization is experienced, possibly causing a controller restart. The system log indicates that “iappd" is consuming the CPU.
104512	✓		When a VSC is configured for non-access controlled 802.1X authentication with a remote RADIUS server, even if the authentication is successful, the controller generates messages similar to this in the system log: `iprulesmgr Discarding RADIUS Packet (Length:'44',Code:'Access-Reject',Id:'87') from RADIUS Server (Ip:'x.x.x.x',Port:'xxxx') due to authentication failure (check shared secret configuration)`
104509	✓	✓	When a wireless client connects to an Active Directory controlled VSC, it shuts down the VSC and indicates a termination of the iprulesmgr process.
104479		✓	APs selects channel 13 even if the channel is explicitly included on the list of non-allowed channels.
104029	✓		Some traffic from a client connected to an access-control VSC (tunneled between the access point and the controller) is detected at the switch where the access point is connected.
103934	✓		(Applies to teamed MSM765zl Controllers.) The management tool always reports a speed of 10Mbps on both the LAN and Internet ports regardless of the actual physical switch module port speed.
103384	✓		When MAC-based authentication is configured for both Local and Remote RADIUS server, the NAS-ID is omitted for the remote RADIUS server.
103346	✓	✓	The **show tech** CLI command causes an internal error.
103192	✓		When a VSC is configured for Mobility Traffic Manager (MTM) (non-access-controlled) and MAC-based authentication is set for both Local and Remote RADIUS servers, the Remote RADIUS server will never be queried even if no match if found in the local RADIUS server.
103062	✓		When mal-formed RADIUS packets are encountered, all wireless client sessions are unexpectedly dropped simultaneously.
102788	✓		(Applies to Japan (JP) versions of MSM320 with an MSM7xx Controller team.) Upon team failover to a team member, the MSM320 shows as having incompatible settings when attempting to re-synchronize with the team member.

ID	MSM7xx	MSM3x4x	Description
102666	✓	✓	(Applies to MSM410, E-MSM430, E-MSM460, E-MSM466.) Clients on different VSCs are wrongly allowed to communicate with each other.
102638	✓	✓	Setting the country to Costa Rica via the CLI causes an `unknown DFS domain` error message to be generated.
102596		✓	(Applies to MSM410, E-MSM430, E-MSM460, E-MSM466.) Automatic channel selection is not working in the 2.4GHz band.
55990	✓	✓	When configuring the maximum number of clients per radio on a VSC, the maximum allowed value is 255 whereas the maximum value for the Access Point group is 999.
55977		✓	APs intermittently restart with the following message in the system log: `info monitord Reset Status - cause=5`
55922	✓		When a less specific static route is configured after a more specific static route has been configured, the controller forwards packets incorrectly.
55742	✓		(Applies to E-MSM430, E-MSM460, E-MSM466 in controlled mode with Mobility Traffic Manager (MTM) and more than 9 VSCs.) When a client associates with an AP not on their home subnet, the client may not get an IP address.
55732	✓		(Applies to E-MSM430, E-MSM460, E-MSM466.) Dynamic VLAN assignment fails, causing user traffic to be placed onto the default network, preventing users from getting an IP address on the correct subnet.
55600	✓		In SOAP, using the GetEthernetAlternateIP method generates error: `The SOAP GetEthernetAlternateIP method returns only the first IP address when a range is used`
55572	✓		When the controller is polled via LLDP for the **Port description** value, the interface alias is returned instead of the Port description.
55556		✓	(Applies to Country=**Japan** (W52&W53&W56) on MSM410, MSM422, E-MSM430, E-MSM460, E-MSM466.) The Auto 20/40MHz channel bonding option for 5 GHz is not available.
55440	✓		When using Active Directory running on Windows 2008R2, access controlled users fail to be authenticated when a team master becomes unavailable and a secondary controller takes over.
55390		✓	(Applies to E-MSM430, E-MSM460, E-MSM466.) Controller based provisioning with local mesh connectivity does not work properly at the AP Group or and Controlled APs levels.
55330	✓		(Applies to non-access-controlled VSCs with 802.1X (Dynamic VLAN) with external RADIUS authentication, and **Allow traffic between all wireless clients** configured.) Wireless clients connected to the same VSC are not able to ping each other.
55301	✓		(Applies to the CLI.) When a leading zero precedes an octet, the network address and team management addresses are incorrectly set.

ID	MSM7xx	MSM3x4x	Description
55118	✓		When both Active Directory and local authentication are selected, neither works.
55041	✓		The controller team name is not available via SNMP.
54612	✓	✓	An 802.1X/WPA2 wireless session cannot be terminated with an SNMP command.
54346	✓		(Applies to Teaming with MSM760 or MSM765zl Controllers.) An unconfigured IP address on the team member egress VLAN allows the access-controlled traffic to be egressed without network address translation (NAT).
54333		✓	APs configured for LED quiet mode still may have blinking LEDs.
54094	✓		Static NAT mappings are incorrectly limited to a maximum of 63 entries by the CLI. The management tool provides for 200 entries.
53749	✓		Users are allowed to add invalid IP Routes.
53110	✓		PCM receives false `ColdStart - Device has crashed ...` messages even when an MSM765zl Controller is fully operational.
52996	✓		Controllers wrongly allow user names to be created with special characters without displaying an error message. Login does not work for user names with special characters.
52971	✓		When the controller DHCP server is configured on **Network>Address allocation>DHCP server configuration>Settings** with no options selected under **Listen for DHCP requests**, DHCP requests will be listened for on all VLANs.
52838	✓		(Applies to Active Directory in Windows Server 2008.) The computer name cannot be used instead of an actual user name.
52829	✓		When a VSC is configured for HTML authentication with remote Active Directory, authentication by the local controller is still permitted.
52713	✓	✓	Under heavy client load, SNMP processes may consume 100% of the CPU, causing the AP to restart.
44394	✓		The local DHCP server in the controller does not reflect the LAN port changes in the gateway address.
43912	✓		When a controller switches from a primary to a secondary RADIUS server, the RADIUS accounting messages from the controller change the configuration source port to use source port 0.
43418		✓	(Applies to E-MSM466 in Monitor mode.) Warning messages similar to the following may fill the system log: `466 radio is set to monitor mode: Warning Kernel WdsLinkMgmtFrameProcess: unexpected probe reply.`
43417		✓	When an E-MSM466 operating in autonomous mode is configured to support monitor mode on its radio, it may become unresponsive.

ID	MSM7xx	MSM3x4x	Description
42381	✓		When configuring an AD (Active Directory) group profile, it is possible to assign a VLAN value so that when a user logs in they will be assigned to this egress VLAN (at the AP). However, this does not work.
41504	✓		The **LLDP port description** value was sending internal port names instead of user configured interface friendly names. The use of friendly or internal names can now be selected on **Network>Discovery protocols >Port description TLV content**.

Known issues

The following known issues are present in this release:

ID	MSM7xx	MSM3x4x	Description
107452	✓	✓	The auto channel feature does not respect the channel exclusion list, allowing the radio to select excluded channels.
105785	✓	✓	When automatic channel selection is triggered at almost the same time on two (or more) neighboring APs, the APs may wrongly be set to the same channel.
102860	✓		Clients roaming to untagged VLANs cannot communicate with the network.
102689	✓		On a controller team, when an interim team manager takes over after the primary team manager becomes inoperative, active access controlled users may experience problems logging in.
66985	✓		(Teaming mode only.) After a software update, some APs may get stuck in the “waiting for manager” state. As a workaround, delete the AP from the configuration and add it again. It is insufficient to just perform a Remove/ Re-discover of the AP.
56028	✓		A controller that has DNS discovery settings defined on the **Controlled APs >> Provisioning > Discovery** page may be unable to synchronize with a team in the following two scenarios: • If the team has different DNS discovery settings configured, the controller will not be able to synchronize. • If the team initially has no DNS discovery settings configured, the controller will be able to synchronize. However, if the DNS settings on the team are then changed, the controller will no longer be able to synchronize.
55755		✓	The E-MSM430, E-MSM460, and E-MSM466 are unable to support more than 125WPA2 clients.
55736	✓		In a controller team, the client event log may be empty for some APs.
55687		✓	(Only 802.11n APs.) When operating in mixed mode (802.11 n/g or n/a), throughput for 802.11n clients may be reduced when 802.11g clients use a lot of bandwidth (for example, when downloading a large file).

ID	MSM7xx	MSM3x4x	Description
44281		✓	(E-MSM430, E-MSM460, and E-MSM466 in autonomous mode only.) The maximum radio power value displayed may be higher than the regulatory limit but the actual output power respects the limit.
43516		✓	(MSM410 and MSM422 radio 1 only.) When operating in 802.11n/a mode and Automatic Power Control is enabled, 802.11n clients can experience low throughput. As a workaround, disable Automatic Power Control.
42979	✓		(Mobility Traffic Manager (MTM) with Opportunistic Key Caching only.) An MTM wireless client sometimes does not get an IP address when a dual-radio AP has both radios enabled with the same VSC and both are part of the mobility domain. As a workaround, do not enable Opportunistic Key Caching in this situation.
42976		✓	(E-MSM430, E-MSM460, and E-MSM466 APs only.) Some 802.11b clients cannot associate with these APs. Ensure that the Multicast rate is a basic rate (1, 2, 5.5 or 11Mbps for 802.11b).
42949	✓		Changes to the Egress VLAN of a group do not change the APs in the group into un- synchronized state, so the APs do not get updated with the changes. As a workaround, move the APs temporarily to a different group, synchronize them, then move them back to the desired group and synchronize them again.
42929		✓	(E-MSM430, E-MSM460, and E-MSM466 in Local Mesh promiscuous mode only.) After the loss of the master, These APs in 802.11n/a mode will not find the new master. The APs must be restarted or power cycled to recover.
42402	✓		(E-MSM430, E-MSM460, and E-MSM466 in a local mesh environment only.) Provisioning local mesh for a downstream AP at the group level causes a radio configuration conflict. As a workaround, provision local mesh for such APs individually directly on each AP.
42376	✓		(E-MSM430, E-MSM460, and E-MSM466 in Monitor mode only.) A group **other than Default** must be used to monitor both the 2.4 and 5 GHz RF bands.
42223	✓		(Teaming mode only.) After a software update, some APs may get stuck in the “waiting for manager” state. As a workaround, delete the AP from the configuration and add it again. It is insufficient to just perform a Remove/ Re-discover of the AP.
42198	✓		(Local mesh only.) If you use a VLAN for discovery, you need to define a separate VLAN for the wireless data traffic.
42190	✓		(Remote Syslog only.) If in the management tool you add a remote log with the name “\” the remote log cannot be deleted except by the CLI or SOAP. Avoid using this name.
42125	✓	✓	A radio cannot be set to monitor mode if it is currently assigned to a VSC using the **Transmit/receive on** setting under **Virtual AP**. As a workaround, first assign the VSC to another radio, then enable monitor mode.

ID	MSM7xx	MSM3x4x	Description
42105	✓	✓	RADIUS profile names must be less than 20 characters in length.
42065	✓	✓	If a VSC is configured to support **Band steering**, you must first disable **Band steering** before changing the **Transmit/receive on** option from **Radio 1 and 2** to a single radio. Failure to do this results in configuration errors in the log file.
42040	✓	✓	If you add an AP to a group that is not bound to any VSC, the AP is never able to synchronize. You must always bind a group to a VSC before you add APs to the group.
42037	✓		The AP Status page incorrectly displays the regulatory domain that is defined for a group. This is only a display issue. The regulatory domain defined for the group is active.
42003	✓	✓	The wireless MIBs do not completely support all new features in this release.
41984	✓	✓	When configuring radio settings, if you modify the value for **Channel** and then change any **Transmit power control** setting without first saving, the setting for **Channel** reverts to its previous value.
41982	✓		When in teaming mode, the **Reserve AP capacity for failover** setting has been removed. You can discard this issue as the changes section in the release notes have a topic devoted to this.
41948	✓		The MSM7xx controllers are vulnerable to DNS Cache Snooping for the DNS service. The DNS service is enabled by default on the LAN interface of the MSM controller and does not run on the Internet interface. The vulnerability allows anonymous users to query the cache using tools such as dig and to gain knowledge about sites that are visited by the local community by inspecting the TTL values found for non-recursive queries found in the DNS cache. The DNS cache option has been left enabled in this release to allow for improved DNS and browser performance. To eliminate the MSM7xx controllers from having this vulnerability, if desired, the DNS cache option may be disabled by disabling the **DNS cache** option on the **Network > DNS** page of the management tool. A discussion of the potential risks of allowing DNS cache information to be queried anonymously is available here: www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf
41931	✓	✓	If an AP is part of a group that is bound to six VSCs, and all the VSCs are configured to broadcast their SSIDs, the AP may only broadcast SSIDs for five of the six APs. If this problem occurs, making any change to the VSC configuration will fix the issue.
41921	✓	✓	(MSM317 only.) When the wired port requires 802.1x authentication, LLDP-MED LLDPDUs are sent on that port before the connected device authentication has passed.

ID	MSM7xx	MSM3x4x	Description
41835	✓		(MSM710 only.) When configured for PPTP, the user may get disconnected when downloading a large file.
41753		✓	(E-MSM430, E-MSM460, and E-MSM466 only.) sFlow samples do not include the extended field for 802.11 Tx information.
41714	✓		Using sFlow with more than 80 APs may cause the controller to respond slowly to SNMP requests. To limit the number of sFlow APs that are being sampled, use the **Advanced Configuration** option on the **Controller >> Tools > sFlow** page.
41710	✓	✓	In controlled mode, for Band steering to be enabled in a VSC bound to this AP type, both of these conditions must be met: • Both radios are in access point mode or access point and local mesh mode. • One radio is set to 802.11n/a and the other is set to 802.11n/b/g.
41708	✓		(MSM325 and MSM320 with Sensor only.) For optimum performance, do not use sFlow on more than 80 APs. Select **Controller >> Controlled APs > sFLow > Advanced Configuration** to select the APs that will be sampled.
41682	✓		When using Mobility Traffic Manager with more than two controllers, if a wireless client roams between two APs managed by different controllers, its traffic may be blocked. The wireless client must re-associate with the network to resume traffic flow.
41650	✓		If teaming is enabled and then disabled, sFlow will not turn on. The controller needs to be restarted for sFlow to work again.
41621	✓		A mobility client that egresses onto its home network locally at the AP that it is associated with will not be shown in the **Controller >> Status > Mobility > Mobility clients** table.
41531	✓	✓	When the country (regulatory domain) for a group is set to a country that does not permit 802.11n on the 5 GHz band, the AP will not be able to synchronize with the controller. This is because radio 1 on these APs defaults to 802.11n 5GHz. To enable these APs to synchronize, disable radio 1 on the **Controlled APs >> Configuration > Radio** list page.
41380	✓		If you enable provisioning under **[***AP name***] > Provisioning** before enabling global provisioning under **Controller >> Controlled AP > Provisioning**, configuration changes will not be applied to the AP. As a workaround, disable provisioning for the AP, synchronize it, re-enable provisioning for the AP, and then synchronize it again.
41366	✓		When you use the **Remove and Rediscover** action on the **Controlled APs >> Overview Discovered APs** page, the APs interfaces are duplicated in sFlow.

ID	MSM7xx	MSM3x4x	Description
41002	✓		(Only when using SNMP to monitor a controller team.) SNMP cannot find the statistics for APs that are attached to a non-manager team member because it thinks they are attached to the manager. A SYSLOG message similar to the following appears: `debug systemagent STATS: GetSystemInfo ConnectRemoteCollector AP=00:03:52:0E:2D:8E error=8 (The remote Id is not fetched)`
40984	✓	✓	In the SNMP system name, using the `%serial_number%` placeholder with any other text will result in the `%serial_number%` placeholder not being converted to its value.
40979	✓		sFlow initialization time takes too long for a large number of APs. With 40 APs the initialization takes approximately six minutes but an hour for 100 APs.
40937	✓		(Only LLDP in Teaming mode.) An AP with a name that includes a placeholder does not display the correct name when the AP is adopted by a team member.
40893		✓	(Only Teaming mode.) A previously-associated client (using WPA2 Enterprise) that is the first to attempt to re-authenticate after a controller failover will not be successful. Subsequent clients attempting to authenticate will not have this issue.
40883	✓		An LLDP agent configured on a port that has Transmit disabled might cause LLDP to become unresponsive on all ports.
40863	✓		(Only Teaming mode.) Two RADIUS profiles with the same uniqueid prevent team members from synchronizing. Avoid this issue by not using duplicate uniqueid values.
40862	✓		When you upgrade to v5.5.0 or higher software or from v5.4.x or lower software, or restore from a configuration saved with v5.4.x or lower software, the software loading wait page remains active indefinitely. This occurs because the web default SSL certificate was changed to “wireless.hp.local” in v5.5.0. Click Refresh in your browser to load the management tool home page.
40818	✓	✓	When a radio is set to Auto Power, the radio always starts with the Maximum allowed value for the specific country and adjusts from that point. Setting the Maximum radio power will have no affect.
40806	✓		(Only Mobility Traffic Manager.) Throughput is low when client traffic is tunneled between two controllers that are not part of the same team.
40737	✓		In some cases, possibly with a slow RADIUS server, 802.1X authentication attempts aborted by the user before completion will accumulate and eventually consume all the available user logins.
40519	✓	✓	APs with layer 2 connectivity to a controller are not able to synchronize if the access-controlled VSC to which they are bound is changed to non-access-controlled.
40354	✓		Controller software cannot be updated from a wireless client using Mobility Traffic Manager.

ID	MSM7xx	MSM3x4x	Description
40306	✓		On a controller team, if a VSC has the **DHCP relay agent** feature enabled with the **Subnet selection** option, the relay does not work properly when the team manager recovers after a shutdown.
40133	✓		When connecting autonomous APs to a controller, traffic is assigned to the default VSC, unless it is on a VLAN, in which case it is assigned to the VSC with matching VLAN ingress definition.
40075	✓		The **VSC >> Overview > User sessions** page may show the incorrect VLAN assigned to the user via RADIUS. This is only a display issue. The correct VLAN is used by the controller to tag the user's traffic.
40071	✓		Wireless mobility (Mobility Traffic Manager and legacy subnet-based mobility) will not work if the controllers in the mobility domain require static routes to reach the primary mobility controller.

40069	✓		To support connection to the public access Interface with Firefox 3.6.3, a valid certificate must be installed and the following access list rules must be defined:
			`factory,allow,ACCEPT,tcp,*.thawte.com,80`
			`factory,allow,ACCEPT,tcp,*.verisign.net,80`

40067	✓		When traffic for a roaming client must be tunneled back to their home network across two controllers, broadcast traffic from the home network will not reach the roaming client.
40038	✓		If you configure your DHCP server to support controller discovery by APs using DHCP Option 43, the APs fail to retrieve the controller addresses if other non-HP options are present after the control IP addresses in the DHCP server configuration.
39992	✓		Under heavy tunneled Access Control traffic, clients sometimes lose connectivity for 2 minutes.
39986	✓		To avoid potential problems with AP synchronization, changing VLAN configuration on a VSC should only be done after all APs are fully synchronized.
39979	✓		On the **Controller >> Status > Mobility** page, the **Networks in the mobility domain** table may show duplicate entries in the **Handler** column.
39946	✓		Worldpay credit card payment does not work.
39914		✓	Revision B MSM410 and MSM422 APs (J numbers end with “B”) do not support 802.11a Turbo mode. Setting a revision B MSM410 or MSM422 to 802.11a Turbo mode and selecting a DFS channel will cause the configuration to be reset.
39906	✓		When using the Mobility Traffic Manager, on the **Controller >> Status > Mobility** page, the Visitors table may temporarily show client devices on the wrong AP/controller. This is a display issue that will resolve itself automatically.

ID	MSM7xx	MSM3x4x	Description
39894	✓		The following configuration settings are ignored when loading a configuration file onto a team manager: • VLANs with static IP addresses • GRE configuration settings • System log filter settings
39888	✓		When a RADIUS profile is added or changed on the controller, the software indicates that all controlled APs need to be synchronized. This is unnecessary and causes wireless traffic to be interrupted for clients not authenticated through RADIUS.
39854	✓		The LLDP dynamic naming feature is not supported when controller teaming is active.
39784		✓	If you plan to connect APs (as slaves) to a controller via local mesh, the APs must first be upgraded to the same software version that is running on the controller. For example, APs running version 5.3.5 cannot connect to a controller as local mesh slaves when the controller is running 5.4.0. Software can only be upgraded on controllers entitled to be upgraded.
39741	✓		If you enable MAC-based authentication in a VSC and a user attempts to login but no user account is defined on the RADIUS server, an error message relating to "iprulesmgr assert" appears in the log.
39699	✓		(Only MSM317.) On an MSM710, if you use the **Swap the LAN and Internet Jacks** option on the **Controller >> Network > Port configuration** page, the swap works but there are no visual indicators to show that the ports are swapped.
39673	✓		VMWare clients are unable to get an IP address when access-controlled VSCs are configured to use DHCP relay.
39661	✓		When a controller is an interim manager, the **Security > Firewall** page is not locked. No changes should be made to an interim manager, only a primary manager.
39648		✓	(Only MSM317.) If wired devices with static IP addresses are connected to the switch ports, the devices are able to communicate with each other regardless of the type of authentication that is enabled on the VSCs bound to the ports, as long as the ports have the same VLAN or no VLAN (untagged).
39644		✓	If you downgrade an AP from 5.3.5 to 5.3.1 and the AP is operating in controlled mode with both radios set to 802.11a on a specific DFS channel, the AP will not be able to synchronize with the controller. To enable the AP to synchronize, go to the radio page and select auto channel or pick a non-DFS channel.
39640	✓		Occasionally during synchronization, a message similar to the following may appear in the log. No action is required: `mapconf: SOAP FAULT: SOAP-ENV:Client "Validation constraint violation: tag name or namespace mismatch in element <Y-MSM:security>`

ID	MSM7xx	MSM3x4x	Description
39622	✓		Specifying an invalid time on the chassis hosting an MSM765zl will result in all controlled APs continuously restarting. Set the correct time on the chassis to avoid this issue.
39557	✓		After a factory reset, restoring a configuration that has WPA2 opportunistic key caching and/or L3 mobility enabled in one or more VSCs will result in a misleading error message being displayed in the VSCs. The error message indicates that validation failed, but fails to indicate the cause of the failure, which is that the required license is not installed. Installing the correct license and restarting the unit corrects the error.

39537		✓	The online help for the CLI command "rcapture" is incorrect. The correct information is as follows:
			Syntax:
			`rcapture -u URI [-c count] -i interface`
			Description:
			Capture data on a port and send it to a file on an FTP server.
			Parameters:
			`URI`: Address of the FTP site and file where the trace will be saved, for example:
			`ftp://user:pass@ftp.mysite.com/trace.pcap`
			`count`: Number of packets to capture.
			`interface`: Interface to trace, where:
			`eth0` = Internet port
			`eth1` = LAN port
			`wvlan0` = wireless port

39489	✓		Users that are a member of a group of the Parent domain cannot authenticate through Active Directory (AD).
39486	✓		Drag-and-drop of APs between groups in the Network Tree does not work in the Mozilla Firefox Web browser.
39467	✓		If you enable several network traces at the same time on different interfaces, you may not be able to stop the traces until you restart the controller.
39432	✓		If you enable/disable NAT on the Internet port (or any VLAN associated with the Internet port), the change does not take effect until you restart the controller.
39422	✓		If you change the IP address of a controller that is part of a mobility domain, L3 mobility does not function correctly until you restart all controllers.

ID	MSM7xx	MSM3x4x	Description
39325	✓		There is a problem configuring RIP in a team environment. The Internet port and LAN port work as expected but PPTP has a problem with respect to not appearing as active on other member controllers. The manager controller is set to active but it shows as passive on the other members.
39287	✓		sFlow does not monitor unicast, broadcast, and multicast counters on any Ethernet interfaces. The values for these counters remain at zero.
39217	✓		If you are using static IP address assignment for either the LAN or Internet port and modify the network mask, the default gateway is lost until the controller is restarted.
39202	✓		If you bind an access control VSC to a switch port you either have to configure your VSC with the Client data tunnel enabled or ensure that you have proper ingress VLANs in the VSCs. Otherwise, after authentication, the client will not go through the proper controller VSC.
39191	✓		If you want to assign the Internet port as the Egress network in a VSC binding, it must have a VLAN. Mobility Traffic Manager currently cannot send user traffic onto the Internet port untagged.
39035	✓		When working with a controller team, the LAN ports on all controllers must be connected via a layer 2 network, even if the LAN ports are not being used by your configuration. This enables controllers to exchange important information.
39025	✓		When DHCP relay is configured with the **Extend Internet port subnet to LAN port** option, and you enable DHCP relay support on a VSC with the **Forward to egress interface** option selected, then you should not select more than one VSC egress mapping with an assigned VLAN.
38973	✓		Assigning 192.168.1.1 to the Internet port can cause problem at startup if the Ethernet port is not being used.
38933	✓	✓	When a radio is disabled, its channel and operating information are still displayed on the AP details page, instead of the radio being shown as disabled.
38882	✓		In a controller team, when you add a static NAT mapping, the mapping definition shows the IP address for the stack manager Internet port. It is important to note that the Internet port address is different for each controller in the team.
38869	✓		When you configure a controller to become the first member and manager of a team, the Filter definitions on the **Tools > System log** page are lost.
38847	✓		The auto-population of the SNMP system name in the web page does not give the a good serial number when you add characters. In the SNMP page the field 'System name:' is auto-filed with the value: “%serial_number%.” If you add characters at the end of this string and execute the SNMP command you should see the serial number plus the characters you added.

ID	MSM7xx	MSM3x4x	Description
38608	✓		sFlow statistics for the MSM317 switch and Ethernet ports may be incorrect for a few moments.
38556	✓		The SOAP sFlow function GetSflowReceiverTableRow returns the wrong timeout value.
38458	✓		The client data tunnel option to **Allow traffic between wired clients and tunneled wireless clients** has been removed from VSCs in this release. If you are upgrading to this release, an equivalent configuration will be created using the new Mobility Traffic Manager feature.
38417	✓	✓	If there are more than 80 APs shown on the Neighbor page, the following message is logged: `Radio 1's node table is full. Too many nodes in the surroundings (max is 256).`
38210	✓	✓	An AP fails to indicate that its configuration is not synchronized when defining provisioning settings. This occurs when you select an AP in the Network Tree and then click **Provisioning > Connectivity**, disable the **Inherited** checkbox, and then define provisioning settings. When you click **Save** the AP should go into the unsychronized state to indicate that configuration changes need to be sent to the AP. However, the AP stays in the synchronized state and must be restarted for the changes to take effect.
38043	✓	✓	When working with a controller team, if you reset an AP, the AP will be discovered with state **Suspicious** and need to be authorized. This is normal. However, if after this a network failure forces the AP to associate with another controller in the team, the AP will incorrectly become **Suspicious** and need to be authorized again.
37834	✓		In a controller teaming environment, the Guest Management Software (GMS) certificate is only installed on the team manager. To avoid problems if the team manager becomes temporarily unavailable, the GMS certificate should be installed on all other controller team members. Manually save and install the certificate as follows: **1.** On the team manager controller, select **Security > Certificate Stores**. **2.** Select the GMS certificate (may be referred to as “VMT”) in the **Trusted CA certificate store** box. **3.** Copy the content from **View certificate** and paste it into a text file with a file name that matches the certificate name. **4.** On all other team member controllers, select **Security -> Certificate Stores**. **5.** In **Trusted CA certificate store**, click **Browse**, select the file created in step 3, and then click **Install**.
37785	✓		When controller teaming is used, the Guest Management Software (GMS) cannot host the WEB pages used for the public access interface. As a work around, you must save your pages directly on each controller or use an external RADIUS server to host the WEB pages.

ID	MSM7xx	MSM3x4x	Description
37672	✓	✓	If the radio is set to operate in 802.11n/g mode, it continues to provide support for 802.11b mode. You can fix this behavior by removing support for the 802.11b modes in each VSC (under **Virtual AP > Allowed wireless rates**).
37576	✓		When a VLAN is configured on the Internet port and the VLAN is used for Ingress mapping in a VSC, and you then reconfigure any VSC, you may lose communications on the LAN port. If this occurs, restart the MSM Controller.
37537	✓		(Only applies to controlled-mode access points in Japan.) Due to regulatory differences for indoor and outdoor access points, one MSM controller must manage indoor access points and another MSM controller must manage outdoor access points.
37507	✓		The management tool incorrectly allows a MSM317 switch port to be bound to an access controlled VSC with **Always tunnel client traffic** enabled. VLANs are not supported by this type of configuration.
37441	✓		Automatic HTML re-authentication works only on the default VSC.
37066	✓	✓	The Axis2 SOAP client toolkit has issues dealing with some SOAP responses. It is recommended that you use a different SOAP client toolkit.
37045	✓		When provisioning a static IP address on an AP, the controller does not validate that the default gateway is on the same subnet as the port. You must make sure the gateway is set correctly.
37038	✓	✓	When configuring the **Allowed wireless rates** option under **Virtual AP** in a VSC, the user can disable support for all 802.11n data rates. If the VSC is only operating on 802.11n, then one non-MSC rate must remain operational or the VSC will not function correctly.
36985	✓	✓	Controlled APs are not able to synchronize with a controller when all of the following occur in sequence: **1.** A VSC is defined with its ingress mapping set to a VLAN on the Internet port. **2.** The controller is restarted. **3.** The ingress VLAN is removed in the VSC. To avoid this problem, remove the VLAN before restarting the controller.
36894	✓		DHCP leases do not indicate the correct VSC when using the **subnet per VSC** feature.
36887	✓		Billing records formats are empty. To fill the fields, select **Reset to Factory Default Format** for each field.
36881	✓		The MSM765 does not support the "shutdown" switch chassis functionality using command: **service <slot> shutdown**. This command will cause a reboot of the MSM765 and not a shutdown. Instead, you can effectively shut down an MSM765zl by removing it from the switch chassis after issuing the **service <slot> shutdown** command.

ID	MSM7xx	MSM3x4x	Description
36879	✓	✓	(Only MSM317.) The MSM317 may generate a **CFG_SYNC_FAILURE** in the log when it synchronizes after a number of configuration changes have been made on the controller. The MSM317 will then restart, apply all changes, and operate normally.
36866	✓		A new default route does not take effect until after restarting.
36854	✓	✓	(Only MSM317.) Applies only when at least one **non-access-controlled VSC** is configured with **Ethernet Switch** as the VSC ingress mapping, and one **access controlled VSC** is configured with a **VLAN** as the VSC ingress mapping.) This message may appear in the system log: `err confighandl Failed to read ingress VLAN information for Virtual Service.` This message should be ignored.
36793	✓	✓	(Only MSM317.) Making any configuration change on an MSM317 (or group of MSM317s) results in all wired 802.1X users on the MSM317 (or group of MSM317s) erroneously having their connections terminated during the synchronization process.
36786	✓		When Address allocation is set to DHCP server, the MSM765zl does not always correctly set the Gateway address to the IP address assigned to the MSM765zl. In some cases, you must set the Gateway IP address manually.
36772	✓		Status information for non-access-controlled wired users does not appear on the **Status > Bridge > Switch** forwarding table.
36767	✓		After performing a software update, the switch chassis log shows the following message: `HPESP: Services zl Module C is rebooting without a proper shutdown`. This is normal and no action is required.
36751	✓		Enabling NAT support on a VLAN only takes effect after a restart.
36739	✓		If Ports 1 to 4 of the MSM317 are bound to a VSC that has WPA enabled with the parameter **Terminate WPA at the controller** selected, then 802.1X wired users that are connected through the port cannot be authenticated.
36728	✓		In a subscription plan, the **Between** option for **Validity period** is off by one hour when system time is set to automatically adjust for daylight savings time. The effective “Between” hour is hour+1.
36622	✓		If a VSC is configured to support WEP with Key source set to Dynamic, **Support static WEP** is displayed, however it is no longer supported.
18151	✓		Client data tunnel configuration options should not appear on a non-access-controlled VSC.